RGICS

RAJIV GANDHI INSTITUTE FOR CONTEMPORARY STUDIES
JAWAHAR BHAWAN, DR. RAJENDRA PRASAD ROAD, NEW DELHI-110001

RGICS ISSUE BRIEF

(April, 2018)

Draft Bill on the **Digital Health Information in Healthcare Security Act 2018 (DISHA)**

RGICS Issue Brief

Draft Bill on the Digital Health Information in Healthcare Security Act 2018(DISHA)

BACKGROUND

The Union Health Ministry has recently released a draft of a proposed law designed to protect health data in the public domain. It is an Act to provide for establishment of National and State eHealth Authorities and Health Information Exchanges; to standardize and regulate the processes related to collection, storing, transmission and use of digital health data; and to ensure reliability, data privacy, confidentiality and security of digital health data. While it mandates the creation of digital health data on every citizen, it also says that any breach of this data can draw a fine of Rs 5 lakh and an imprisonment of up to five years, this ten-member National Digital Health Authority of India is designed to become the bulwark for the National Health Protection Mission 2018, the ambitious health programme that aims to cover 10.74 crore families against annual medical expenses of up to Rs 5 lakh.

Information technology analysts have suggested that the Bill is a good step to advance the rights of citizens and bring in coherence in managing health data, which is scattered across paper files and digital formats at various facilities. As per the National Health Policy of 2017 a regulatory authority would be constituted to manage health data and this Bill is a move to make that a reality. With this Bill, the government is looking to integrate eHealth better into its systems along with data protection. However the medical fraternity has greeted the bill rather warily, pinpointing anomalies and seeking clarity on various counts. The Indian Medical Association (IMA) is in the process of discussing the bill and plans to file its response to the ministry after April 15.

PART II. KEY FEATURES OF THE BILL

Hospitals in India started using EMRs as the preferred method of storing patient information as it helps with easier access to medical information in order to aid public policy, the legal framework supporting such a governance initiative, specifically relating to data security and privacy, remained inadequate. Currently the framework envisaged for governing EMRs in India is the draft Electronic Health Record Standards released by the Ministry of Health and Family Welfare (MoHFW). Some of the criticisms of these standards include- an unclear scope of coverage, uninformed consent, lack of clearly defined timelines for accessing patient records, the failure to include unique identification information such as URLs and IP addresses as sensitive information and an ambiguity in defining the scope of 'personal health information. To enforce privacy and security measures for digital health data, the Centre has drafted a law which will eventually become the backbone of the National Health Protection Mission that makes any breach punishable by imprisonment along with a fine. Following are the key features of the Bill[1]:

A. Ownership of digital health data

The digital health data generated, collected, stored or transmitted will be owned by the individual whose health data has been digitized. In addition, a clinical establishment or Health Information Exchange shall hold such digital health care data while there will be a state level — State Electronic Health Authority — and a national level — National Electronic Health Authority. These authorities are tasked with the objective to protect the privacy, confidentiality and the security of the owner's digital health data.

B. Rights of the data owner

The owner of digital health data shall have the following rights:

Consent

i. The owner has the right to privacy, confidentiality, and security of their digital health data" and the right to refuse consent for the generation and collection of digital health data by clinical establishments and entities," subject to certain exceptions;
ii. The right to give, refuse or withdraw consent for the storage and transmission of digital health data, as well as to refuse consent to access and disclosure, with certain exceptions;
iii. The right to require their explicit prior permission for each instance of transmission or use of their digital health data in an identifiable form;

---

i. [1]Read the full Bill at file:///C:/Users/RGICS/Desktop/R_4179_1521627488625_0.pdf

iv. The right to prevent any transmission or disclosure of any sensitive health related data that is likely to cause damage or distress to the owner;

Transparency

i. The right to know the clinical establishments or entities which may have or has access to the digital health data, and the recipients to whom the data is transmitted or disclosed;
ii. The owner of the digital health data shall have a right to access their digital health data with details of consent given and data accessed by any Clinical Establishment/Entity;
iii. The right to be notified every time their digital health data is accessed by any clinical establishment

Ratification

The rights to rectify without delay, from the respective clinical establishment or health information exchange or entity, any inaccurate or incomplete digital health data.

Sharing of data

i. The right to ensure that in case of health emergency, the digital health data of the owner may be shared with their family members;
ii. The right not to be refused health service, if they refuse to consent to generation, collection, storage, transmission and disclosure of their health data;
iii. Protection: The right to seek compensation for damages caused by a breach of digital health data.

C. Data collection and defining personally identifiable information

i. **Notice and consent:** A clinical establishment may, by consent from the owner, collect the required health data, after informing the owner of their rights. Also, the establishment has to furnish a copy of the consent form. If any other entity collects any digital health data has to be the custodian of such data, and is duty bound to protect the privacy, confidentiality and security of such data.

ii. **Consent in case of incapacitation/incompetence:** When an individual is incapacitated or incompetent to provide consent, proxy consent may be taken from a nominated representative, relative, care giver or such other person.

iii. **In case of sensitive information**: The patient has the right to prevent any transmission or disclosure of any sensitive health related data that is likely to cause damage or distress to the owner[2]

D. Purpose of collection, storage, transmission and use of the digital health data

i. Gain personally identifiable information in order to improve the coordination of care and information among hospitals, laboratories, medical professionals, and other entities through an effective infrastructure for the secure and authorized exchange of digital health data;
ii. To improve public health activities and facilitate the early identification and rapid response to public health threats and emergencies, including bio terror events and infectious disease outbreaks;
iii. To promote early detection, prevention, and management of chronic diseases;
iv. To carry out public health research, review and analysis, and policy formulation;
v. To undertake academic research and other related purposes

E. Accessing digital health data

i. The Insurance companies are not allowed to access the digital health data of persons who seek to purchase health insurance policies or during the processing of any insurance claim. For the purpose of processing of insurance claims, the insurance company shall seek consent from the owner to seek access his or her digital health data from the clinical establishment to which the claim relates. So while the position on insurance companies is ambiguous as per the NeHA, yet it does allow the healthcare companies that sell insurance to access it with informed consent. **Further the Bill has not defined the rules/procedures in this regard; in case of insurance claims, what happens if the patient does not give consent to the healthcare provider but only to the insurance company, and vice versa? Will the insurance payout be denied if consent not given?**
ii. All clinical establishments and health information exchanges on other hand need to maintain a register in a digital form to record the purposes and usage of digital health data accessed. **However there is no mention of a third party audit of the data trail.** It is not clear if the records will also have to be maintained in the physical format too.
iii. Digital health data may be accessed by the clinical establishment, on a need to know basis without any authority to do so. **The Bill although does not define what is "need to know basis" nor will the patient be informed what has been done with his/her medical record and how will it benefit him/her in the future.**
iv. Government departments through their respective Secretaries, may submit request for digital health data in **deidentified/ anonymized form**, to the National Electronic Health Authority.

[2] Sensitive health-related information' means information, that if lost, compromised, or disclosed, could result in substantial harm, embarrassment, inconvenience, violence, discrimination or unfairness to an individual, including but not limited to, one's physical or mental health condition, sexual orientation, use of narcotic or psychotropic substances, consumption of alcohol, sexual practices, Human Immunodeficiency Virus status, Sexually Transmitted Infections treatment, and abortion.

v. In case of an emergency certain digital health records are allowed for immediate use to a clinical establishment, including information related to allergies, drug interactions and such other information as may be specified. **The Bill although hasn't defined "emergency" in this case**.

vi. **In case of death** of the owner of digital health data, the legal heirs are the representative of such owner may have access to such data, unless expressly barred by the owner. Provided further that in case of death of the owner, the National Electronic Health Authority shall use the digital health data only in anonymized form.

1. **Penalties for breach/serious breach**

i. Any person who commits a breach has to pay damages by way of compensation to the owner of the digital healthcare data in relation to which the breach took place. **However there is no process defined in order to identify who exactly committed the breach and how can it be proved at which level the breach took place. While there are penalties laid out for committing a serious data breach, the Bill does not provide provisions how the authority shall track unauthorised/ serious data breach and inform the purpose for such data breach, if it happens.**

ii. Any person who commits a serious breach of health care data will be punished with imprisonment, of 3 to 5 years; or fine, which shall not be less than five lakh of rupees.

iii. If anyone is caught fraudulently or dishonestly, obtaining the digital health information of another person, which he/she is not entitled to obtain will be punished with imprisonment for a term which shall extend up to one year or fine, which shall be not less than one lakh rupees; or both.

iv. Where a company contravenes this act, will be proceeded against and punished accordingly. Provided that the contravention took place without the company's knowledge or he exercised all due diligence to prevent the commission of such contravention. It has been clarified that a company may be prosecuted notwithstanding that the prosecution or conviction of any legal juridical person shall be contingent on the prosecution or conviction of any individual. **However, there is no such provision or requirement mentioned for the companies to inform individuals if their personal information has been compromised as a result of a data breach. In fact, for any effective data protection framework, this is a fundamental SOPs that need to be clearly defined while framing a framework that protects and promotes rights of the persons who own the data.**

PART III. KEY ISSUES

Creation of a data protection authority as a regulator managed by the State could lead to serious consequences that include violation of civil liberties: This Bill goes on to propose setting up a National Digital Health Authority" a statutory body for promotion/ adoption of these e-Health standards hardly taking into considerations the criticism. Although setting up of security safeguards for medical information is a welcome step amid the growing threat of electronic data misuse with incidents of sensitive data lying unprotected, and data theft and hacking becoming routine, there could be serious consequences of putting so much power in the hands of one authority that will be working under the government of India. Not only will this regulator have the power to inspect records and data in the guise of data audits, bestowing on them the authority to create a data protection authority that will have the powers to punish both public and private sectors across the country for any violation of privacy or data protection laws. Further the Bill excludes courts from taking cognizance of offences under the legislation, requiring that the authority that is responsible for taking consent to prosecution for any action to be taken under the legislation. This part of the Bill completely undermines all the safeguards that exist within it, since citizens cannot access these safeguards without co-operation from the authority which is arguably in a position of conflict of interest.
For instance, the recent case of data leak from the NaMO App is a matter of grave concern, as these instances raise concerns that the initiatives on technology and governance by the Indian government are removed from the concerns of the citizens and implemented with almost no explanation.[3]

Without strengthening the internet connectivity in India, the government may not be able to achieve its goal of collecting, managing and securing medical health records electronically: Rural India lags behind urban areas in not just Internet penetration but also in Internet access for online financial transactions due to lack of electricity and poor network quality, as per a study by Internet and Mobile Association of India (IAMAI). Only 16% of rural users access the Internet for financial transactions, while in urban areas 44% users access the Internet for this purpose, according to the report. Further lack of electricity to charge devices, poor network quality and affordability of Internet service packs are the reasons for such behavior and unless this trend is reversed, usage purposes will remain skewed and off take of digital payments will remain restricted.

Linking of NeHA with the NHPS will require stringent procedures to avoid exclusion: In such a case, if the government wishes to link the NeHA with the New Health Protection Scheme to promote cashless benefits to the 40 % targeted population who belong to the below poverty line the government needs to ensure that beneficiaries are well informed about the idea of consent , the benefits of giving in their consent and that in no way internet access and usage is denied to the people especially in the rural areas.

[3] https://www.nytimes.com/2018/04/03/opinion/india-data-privacy-biometric-aadhar.html

Lack of strong consent mechanism: While the Bill does provide for seeking consent for collecting, storing and managing health records, the Bill does not specify that this must be informed consent with an 'opt out' mechanism and does not specify the manner in which such consent should be sought. This leaves it in the hands of the government and possibly the third requesting entity to determine the form of consent that is to be taken. This could result in ambiguous, misleading, or inconsistent consent mechanisms being used. Most privacy laws promote autonomy by creating a threshold condition that requires the data controller to seek the consent of the individual before collecting personal data from him. However, this power has existed in name alone as the consent that the individual provide is not meaningful and, at best, does lip service to the notion of autonomy (in case of Aadhar).Therefore, the government needs to focus our efforts on ensuring that the patient has every opportunity to exercise his autonomy after the data has been collected.

Not clear who controls electronic health records: There is still no clarity on the manner in which the information is to be generated or stored, According to the draft, the digital health data may be generated, collected, stored and transmitted by clinical institutions as well as by health information exchanges (HIEs) but the process including the time period for which it will be stored, has not been specified. In addition to this, it is not clear who will transmit the digital health data, the clinical establishment or HIEs, and it what stage will it be anonmysied. Also not clear why both the clinical establishment and HIEs have been vested with the right to alter data, although this cannot be done without intimating the patient. If one end makes the change without the knowledge of the other, it is bound to impact the veracity of data and have implications for both the patient and the policy making/user groups. In fact, the government should take responsibility of data security as the HIEs will be operated mostly by government machinery rather than clinical establishments or healthcare providers. Moreover, since a large number of States are yet to adopt the Clinical Establishment Act, collecting medical records could be delayed**.**

Linking of Aadhar with the health records contravenes existing provisions of Aadhar Act and could lead to a possible invasion of an individual's privacy by forcing patients to provide blanket consent for use of their medical data: The new law on health privacy will provide for collecting Aadhar numbers linked to medical records. In fact, the National Health Policy also states that the government will be exploring the use of "Aadhar" (Unique ID) for identification and creation of registries. So while the draft Bill provides the data owner the right to give or refuse consent for the generation and collection of digital health data by clinical establishments and entities, the inclusion of Aadhar may however give excessive power to the government over the data as the government today is linking an increasing number of benefits and government services to the 12-digit biometric-based Aadhar number for Indians, that creates a possibility of leakage. In addition to this, the Aadhar Act does not allow collecting medical history as part of the demographic information. Further, research has proved that patients can be re-identified, without decryption, through a process of linking the unencrypted parts of the record with known information about the individual. These de-identification methods were bound to fail, because they are trying to achieve two inconsistent aims: the protection of individual privacy and publication of detailed individual records. Anonymization is very unlikely to work for other rich datasets in the government's care, like census data, tax records, mental health records etc. So

while the ambition of making more data more easily available to facilitate research, innovation and sound public policy is a good one, there is an important technical problem to solve: there is no real solution for publishing sensitive complex individual records that protects privacy without substantially degrading the usefulness of the data.[4]

The Bill does not address the issue of privacy of data of those patients whose data is already with the Ministry: Since 2016, the Ministry of Health had started to collect Aadhar numbers of those seeking treatment at government hospitals and medical colleges. The government has not addressed the confidentiality of the patients and their data. Moreover, since there have been past incidents where health data has been linked, if the new section of compensation by the government/entity will be applicable to them. Moreover, neither practices/action plans are talked about for increasing awareness 'for the patients and the practitioners are particularly of their rights and responsibilities.

The standards need to be made stricter with regard to accessing health data even by government authorities: The standards need to be made stricter as they mention that all recorded health data will be available to health care service providers on an "as required on demand" basis, and has not been limited to healthcare purposes.

Lack of grievous redressal mechanism: There is no grievance mechanism provided for in the Act through which a complaint against the Authority could be filed in the event that the data collected by the Authority is misused. Similar concern was been raised in the case of the Aadhar Act which too contains no provisions to address privacy concerns. Thus any legal action against any misuse or theft of Aadhar data can only be initiated by UIDAI, leaving citizens with no legal recourse should a breach occur. This is a clear case of conflict of interest as it gives exclusive power to the very authority that is responsible for the security and confidentiality of identity information and authentication records.

[4] https://pursuit.unimelb.edu.au/articles/the-simple-process-of-re-identifying-patients-in-public-health-records

PART IV-CONCLUSION

The proposed HDPSA (Health Data Privacy and Security Act) 2018 which has been presented by the Health and Family Welfare department of the Union Government draws a lot from the HIPAA (Health Insurance Portability and Accountability Act) 2009 of USA. However, The Omnibus Final Rule of HITECH Act that has been published in March 2013 has made changes to the earlier HIPAA rule for the Covered Entities, Business Associates, access to medical records and information regarding registering complaints against the healthcare providers in case of data breach/misuse of data. Unfortunately the ownership rights of patients provided under a data protection law based on accountability have been completely ignored in the DISHA draft Bill.

Some of the key provisions ignored by DISHA Draft Bill and their implications include:

New rule under HIPAA	Explanation	Comment
Appointing a Business Associate	A "**business associate**" is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the **business associate** to protected health information.	A business associate works as a third-party contractor for or on behalf of a healthcare organization or covered entity in order to protect any sensitive health information. (Earlier managing security of PHI fell upon the covered entity[5] in the form of Business Associate agreement).
Process to identify a breach	In order to determine whether a breach has occurred (and whether a breach notification is required), a Covered Entity or Business Associate must conduct a risk assessment to determine whether the use or disclosure of PHI in question poses a significant risk of	This process is useful to identify who committed the breach and at what stage has the breach taken place. Accordingly, the new data protection law should have offered a mechanism by which harm can be detected early enough to head off significant adverse

[5] Covered entities are defined in the HIPAA rules as (1) health plans, (2) **health care clearinghouses**, and (3) **health care providers** who electronically transmit any health information in connection with transactions for which **HHS** has adopted standards. For example Hospitals, Clinics, individual Practicing Physicians

	financial, reputational, or other harm to the individual.	consequences.
The right to receive a notice of privacy practices	Patients have the right to receive a notice explaining how a provider or health plan uses and discloses their health information. In fact, The notice of privacy practices will provide information about who to contact with privacy questions and how to complain.	In this way, the patient has more control over his/her medical records and has the right to opt out in case, he/she does not want the healthcare provider to access their data.

Recent incidents of data leak from Aadhar, Facebook and Cambridge Analytica**,** raise several deeper questions about our relationship with technology, radical changes in ideas of privacy and ownership of the self, and the implications of the new data-driven order for democracy and politics. In the absence of a clear framework to deal with data protection and privacy issues and with increasing digitalization it is essential for India to formulate a comprehensive new law which can balance the privacy concerns of citizens, protect business systems and at the same time regulate the data ecosystem, especially when related to the sensitive issues of health.

PART V. BACKGROUND INFORMATION/REFERENCE DOCUMENTS

i. https://scroll.in/pulse/833190/aadhaar-in-health-records-legal-experts-and-government-divided-over-who-will-own-data
ii. https://punemirror.indiatimes.com/pune/civic/digital-health-data-bill-met-with-caution-by-medical-assns/articleshow/63550686.cms
iii. https://www.moneycontrol.com/news/business/why-does-the-clinical-establishment-act-remain-mostly-on-paper-2530741.html
iv. https://www.firstpost.com/tech/news-analysis/central-govt-invites-comments-on-draft-digital-health-security-law-by-21-april-data-breach-can-bring-a-rs-5-lakh-fine-and-a-jail-term-4407155.html
v. https://thewire.in/law/without-data-security-and-privacy-laws-medical-records-in-india-are-highly-vulnerable
vi. https://healthitsecurity.com/news/healthcare-data-privacy-security-concerns-hinder-digital-adoption
vii. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5522514/
viii. https://thewire.in/tech/data-protection-law-regulator-india
ix. https://www.bloombergquint.com/law-and-policy/2018/04/07/india-to-spend-rs-16717-crore-on-modis-health-insurance-plan-in-two-years
x. https://scroll.in/pulse/869000/interview-insurance-should-not-be-the-only-financing-model-for-public-healthcare-in-india
xi. https://www.livemint.com/Opinion/3GqDnEIYPxbuzwJuT4dkaM/Is-the-National-Health-Protection-Scheme-good-public-policy.html
xii. https://timesofindia.indiatimes.com/city/pune/ima-picks-holes-in-disha-draft-bill-writes-to-ministry/articleshow/63873174.cms